Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 10 February 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Washington Post reports cybersecurity experts say an increasing number of private or putatively secret documents are online in out−of−the−way corners of computers all over the globe, leaving the government, individuals, and companies vulnerable to security breaches. (See item 4)
- The Associated Press reports several Asian regions have instituted temporary bans on poultry imports from all or parts of the United States following discovery of bird flu in Delaware. (See item 15)
- Computerworld reports another Mydoom variant, known as Mydoom.C or SyncZ, appears to be scanning the Internet for systems already infected by the original Mydoom. (See item 24)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *February 09, CNS* — **High winds could down power lines. The National Weather Service says gusts of wind over the next four days in southern California could break tree limbs and cause power outages.** The winds will be highest in the mountains and valleys of San Bernardino and Riverside counties, with gusts reaching 70 miles−per−hour. Winds will also be strong in Orange County, but not as powerful as in the eastern counties.

Source: http://abclocal.go.com/kabc/news/020904_nw_winds.html

2. *February 09, Associated Press* — **Ministers urge OPEC to curb production. Fearing a springtime glut in crude supplies, several Organization of Petroleum Exporting Countries (OPEC) oil ministers urged the group's members Monday to slash overproduction at once and to consider approving cuts in their output quotas as early as next month.** Representatives of OPEC argued for better self−restraint, at the minimum, in the hope of buttressing oil prices, as they arrived in Algiers, Algeria, ahead of a meeting Tuesday to review the group's oil policy. Although OPEC often calls on its members to curb overproduction, its belief that prices could plunge when seasonal demand dips during the April−June quarter gives the message an unusual urgency this time. OPEC's 11 members pump about a third of the world's oil.
Source: http://www.washingtonpost.com/wp−dyn/articles/A25920−2004Feb 9.html

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *February 09, Federal Computer Week* — **Army's Future Combat Systems at the heart of transformation.** In October 1999, Eric Shinseki, then the Army's chief of staff, launched a bold initiative to make forces lighter, modular and rapidly deployable. **Shinseki's goal was to field a brigade in four days, a division in five days and five divisions in 30 days. Working with the Defense Advanced Research Projects Agency, four contracts were awarded in May 2000 to four industry teams to develop Future Combat Systems (FCS) designs.** On May 14, 2003, the Defense Acquisition Board approved FCS' next acquisition phase, and the department approved it on May 31, 2003. In August 2003, the two main private contractors chose and awarded contracts to 21 companies to design and build FCS' platforms, hardware and software, and will oversee the program through DOD's systems development and demonstration phase.
Source: http://www.fcw.com/fcw/articles/2004/0209/pol−army−02−09−04. asp

[Return to top]

Banking and Finance Sector

4. *February 09, Washington Post* — **Online search engines help lift cover of privacy. Cybersecurity experts say an increasing number of private or putatively secret documents are online in out−of−the−way corners of computers all over the globe, leaving the government, individuals, and companies vulnerable to security breaches. At some Websites and various message groups, techno−hobbyists are even offering instructions on how to find sensitive documents using a relatively simple search.** Though it does not technically trespass, the practice is sometimes called "Google hacking." In the decade they have

been around, search engines like Google have become more powerful. At the same time, the Web has become a richer source of information as more businesses and government agencies rely on the Internet to transmit and share information. All of it is stored on computers called servers, each one linked to the Internet. For a variety of reasons −− improperly configured servers, holes in security systems, human error −− a wide assortment of material not intended to be viewed by the public is, in fact, publicly available. **Once Google or another search engine finds it, it is nearly impossible to draw back into secrecy.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A24053−2004Feb 8.html

5. *February 08, Associated Press* — **Governor signs identity theft bill.** Wisconsin Governor Jim Doyle has signed into law a bill that removes personal information from data filed online with a state agency to help prevent identity theft. **State officials said the new law means that individual Social Security numbers or employer identification numbers would no longer be filed online with the state Department of Financial Institutions when state residents borrow money and secure the loan with personal property.** The online filings had made the information susceptible to computer hackers who steal identities, officials said.
Source: http://www.gmtoday.com/news/politics/state/topstory176.asp

6. *February 04, Washington Square News (NY)* — **Colleges react to identity theft. Technological snafus and security breaches are quickly becoming a growing problem among the nation's collegiate computer systems, leaving in its wake a slew of identity theft horror stories. Many schools including Rutgers University, Texas A&M, the University of Georgia and Boston College, recently reacted to security lapses by ridding their student ID systems of Social Security numbers.** The most egregious leak of private information took place in late January, when University of Georgia officials found that hackers had penetrated the school's Website, gathering the personal information −− including Social Security and credit card numbers −− of 31,000 students and applicants. The University of Georgia and other schools are part of a trend among U.S. schools to abandon Social Security number−based ID systems. Some are converting to a system that selects nine−digit ID numbers randomly, and others are using a combination of student initials and numbers. Although students at many universities may opt to use non−Social Security numbers as IDs, Ken Iuso, registrar at Rutgers University, stressed that colleges are required by the federal government to keep Social Security numbers on record, even if they are not used to identify students.
Source: http://www.nyunews.com/news/campus/6640.html

[Return to top]

Transportation Sector

7. *February 09, Department of Transportation* — **Secretary Mineta introduces new air traffic control system in Milwaukee.** Department of Transportation Secretary Norman Y. Mineta visited Mitchell International Airport to introduce its new air traffic control technology and reiterate the Administration,s commitment to improvements aimed at reducing airspace congestion nationwide. **During a visit to the airport's air traffic control facility, the Secretary said that Mitchell International is the nation's first airport to use a new runway safety tool known as the Airport Surface Detection Equipment Model−X (ASDE−X) system that will help reduce costly air traffic delays and maximize safety for passengers**

traveling into and out of the airport. “This important new technology will help minimize costly air traffic delays and maximize safety for passengers at Mitchell International,” said Secretary Mineta. “A strong economy depends on a strong aviation system.” This year, the Department of Transportation will deploy ASDE−X at four other major airports in Orlando; St. Louis; Charlotte, North Carolina; and Providence, Rhode Island, with 12 more installations planned in Fiscal Year 2005. And, in the next two years, the Department expects to bring STARS to 16 more airports around the country.
Source: http://www.dot.gov/affairs/dot1204.htm

8. *February 09, The Trucker* — **Authorities monitor trucker Websites, radio stations in ricin case. FBI agents and Department of Defense (DoD) officials recently arranged for the host of the "Truckin' Bozo" radio show to publicize the $100,000 reward for information on ricin−laced letters.** Radio show host Dale Sommers was asked to broadcast the reward information on three separate occasions, the Washington Post reported February 6. According to the Post article, authorities also have been studying various trucking companies to see if they can find the person calling himself or herself "Fallen Angel." A package containing ricin and a threatening letter was found in the postal facility serving the Greenville−Spartanburg International Airport in October 2003 and in November a similar letter and vial of ricin were found at a White House postal facility. The writer of both letters, "Fallen Angel," claimed to be the fleet owner of a tanker company who threatened to start dumping ricin if DOT didn't rescind the new Hours of Service rules. Authorities apparently have found no connection between the 2003 ricin letters and the ricin found Febuary 2 in the fourth−floor mailroom that serves Senate Majority Leader Bill Frist's office.
Source: http://www.thetrucker.com/stories/02_04/0209_ricin_appeal.ht ml

9. *February 09, The Seattle Times* — **Coast Guard challenged by terrorism risk.** As the Coast Guard tackles its new mission of protecting America from terrorist attack, one of the tools it needs is a radio frequency to help monitor the movements and cargo of thousands of ships that enter the nation's ports each year. **However, the Federal Communications Commission — over the Coast Guard's objections — sold the frequency at auction to a private company in 1998 for $6.8 million.** The squabble over the radio frequency is just one of the obstacles the Coast Guard faces between now and July 1, its deadline for enforcing new anti−terrorism rules mandated by the federal Maritime Transportation Security Act of 2002. **About 3,200 of the potential targets are on shore: oil refineries, nuclear−power plants, liquid−natural−gas facilities and hundreds of other waterfront sites that use or store hazardous materials. The 8,500 others are on the water: ferries that carry tens of thousands of commuters to work in cities from Seattle to New York, barges and cargo ships that crisscross U.S. harbors and inland waterways, oceangoing tankers and freighters that bring in everything from oil and fertilizer to automobiles and bananas.** Oceangoing vessels are of special concern. Container ships alone bring 16 million boxcar−sized containers a year to U.S. ports, and 95 percent of them are unloaded without ever being inspected.
Source: http://seattletimes.nwsource.com/html/nationworld/2001853485_ports08.

10. *February 09, San Francisco Chronicle* — **San Francisco, Oakland ports to get high−tech security.** Next−generation radiation−detection equipment −− designed to find a terrorist "dirty bomb" hidden among forests of cargo containers −− will be deployed at the ports of Oakland and San Francisco as early as this summer, a top federal official said Friday, Februaary 6. **The**

two Bay Area seaports will be the first ports in the nation to use the high−tech devices, which are analogous to sophisticated X−ray machines. The big challenge is getting money for mandatory programs," Ray Boyle, the Port of Oakland's general manager of maritime, told the gathering at Wells Fargo HSBC Trade Bank. "We have had $16 million in unreimbursed security costs since 9/11: $5 million at the seaport and $11 million at Oakland International Airport."
Source: http://www.sfgate.com/cgi−bin/article.cgi?file=/chronicle/archive/2004/02/07/BUGMD4R6M91.DTL

11. *February 09, Baltimore Sun* — **Mass transit moving into digital age.** Imagine being at a bus stop and knowing how long it will be before your ride arrives. That and other information pertinent to riding mass transit will be available to the Maryland Mass Transit Administration's (MTA) bus riders by 2006, when a network known as the NEXT System is installed in the Baltimore area, Gov. Robert L. Ehrlich Jr. announced. **The NEXT System is an integrated network that uses global positioning satellite systems and wireless technology to allow the MTA to know where each bus or train is at any given time and translate that information into real−time messages that can be read by customers at a bus stop or train platform.** Riders at 200 of the region's busiest bus stops will be able to see schedule information and learn when their bus will reach their stop. The system also monitors the mechanical condition of a bus while it is operating, allowing mechanics to spot a potential problem before it causes a breakdown. The MTA's current plans call for the technology to be in place by the end of 2006.
Source: http://www.baltimoresun.com/news/local/bal−next0209,0,4420584.story?coll=bal−local−headlines

[Return to top]

Postal and Shipping Sector

12. *February 09, Associated Press* — **Fumigation successful, Postal Service says. Fumigation of the Hamilton, NJ, mail distribution facility that handled at least four anthrax−laced letters more than two years ago successfully eliminated all traces of the bacteria, U.S. Postal Service officials announced Monday.** Thomas G. Day, vice president of engineering for the Postal Service, said he expects the building will reopen by the end of the year, and possibly as soon as late summer. **Day estimated the cleanup cost to be $80 million so far for the Hamilton site, a figure that will continue to grow as the facility is refurbished.** Eddy Bresnitz, who chaired a state committee that monitored cleanup, said that after the two−day treatment with chlorine dioxide last fall, 4,777 surface and air samples were taken in the building. None showed the presence of anthrax, he said.
Source: http://www.newsday.com/news/local/wire/ny−bc−nj−−anthrax−postalfac0209feb09,0,31272.story?coll=ny−ap−regional−wire

[Return to top]

Agriculture Sector

13.

February 09, Associated Press — **Vietnam reports foot−and−mouth disease. Some 1,400 cows, buffalos and pigs have been infected with foot−and−mouth disease in central Vietnam, provincial officials said Monday.** The disease was initially reported in central Quang Nam province in late December, and local auhtorities have destroyed 84 infected pigs, said Nguyen Xuan Phuc, chairman of the provincial People's Committee. However, infected cows and buffalos are being treated and some of them have recovered, he added. Phuc did not explain why the infected pigs were targeted for destruction. The remaining animal herds have been vaccinated, and the provincial government has imposed a ban on transportation and sales of the animals from the three infected districts, he said. **Central Quang Ngai and Kon Tum provinces have also reported outbreaks of foot−and−mouth disease, Phuc said.**
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/791157 8.htm

14. *February 09, Oster Dow Jones Commodity News* — **USDA ends BSE investigation. The U.S. Department of Agriculture (USDA) announced that it has wrapped up the investigation into the December discovery of a dairy cow infected with bovine spongiform encephalopathy (BSE), in Washington state.** USDA spokesman Ed Loyd said "the active part of the investigation" has been completed. The USDA quickly discovered and proved, throgh DNA testing, that the infected cow had been imported from Canada along with 80 other herdmates. The hunt for those 80 animals that came over the border more than two years ago has ended. As of Friday, the USDA said 28 have been found. The importance of these cattle, according USDA's chief veterinarian Ron DeHaven, is that they likely fed together as young calves and feed, if it contains infected ruminant material, is believed to be the only way mad−cow disease is spread.
Source: http://www.agprofessional.com/show_story.php?id=23481

15. *February 09, Associated Press* — **More nations ban U.S. poultry. Several Asian regions have instituted temporary bans on poultry imports from all or parts of the United States following discovery of bird flu in Delaware.** The state ordered the slaughter of some 12,000 chickens Friday since the discovery of the strain, which is milder than the one ravaging several Asian countries. **South Korea, Malaysia, and Japan have barred all U.S. imports, while Hong Kong is only restricting Delaware products.** The U.S. is Japan's fourth−largest supplier of poultry and poultry products. The United States is not a significant poultry supplier for Malaysia.
Source: http://www.channeloklahoma.com/health/2832451/detail.html

16. *February 09, Associated Press* — **Contaminated sorghum targeted by inspectors. Mexican agricultural officials trying to stop tainted sorghum seeds from crossing out of Texas say more than 20 percent of the crop is contaminated with ergot.** Mexican farmers need the sorghum, one of two cereal grasses mainly cultivated for stock feed in Mexico. But they fear losing their crops to disease. "Ergot can destroy harvests if it appears before sorghum flowers bloom," Leon de los Santos, an agricultural inspector with Senasica−Sagarpa, a Mexican agricultural government agency, said Ergot is a disease that affects the production of the seeds, if pollen production is poor, according to the Kansas Grain Sorghum Producers Association. The group said the disease was found in Texas in 1997. In Brazil, an epidemic of ergot in 1995 covered 300,000 square miles in a week.
Source: http://www.miami.com/mld/miamiherald/news/breaking_news/7910 466.htm

[Return to top]

Food Sector

17. *February 09, Agricultural Research Service* — **New database helps monitor food pathogens.** The world's largest online database of information on how pathogenic bacteria respond to different environmental conditions in food has been established by scientists with the Agricultural Research Service and the United Kingdom's Institute of Food Research. **The database, ComBase, is designed to help make risk assessments and model development easier.** ComBase software facilitates research cooperation among scientists studying predictive microbiology. **This growing field estimates the behavior of microorganisms in response to environmental conditions, including food production and processing operations from the farm to the table.** Using the database, scientists can enter data such as the temperature, acidity, and available water, and then retrieve all records that match the search criteria.
Source: http://www.ars.usda.gov/is/pr/2004/040209.htm

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

18. *February 09, Washington Post* — **Old, new diseases taking hold. Epidemiologists and public health specialists say that diseases formerly thought to be nearly eradicated have gained a tenacious foothold in the early 21st century.** The world never before has had so many medicines, vaccines, or detailed knowledge about everything from rare disorders to sanitary food preparation. A complex combination of factors have joined forces to "weaken the herd immunity," say public−health analysts. The widespread use of antibiotics in medical treatment and meat production has weeded out the germs they were created to destroy, clearing the way for new microbes and superviruses, which are drug−resistant. AIDS and malaria significantly weaken the immune system, making victims vulnerable to tuberculosis and other infections, and compromising society's general resistance to plague or other germs. Humans are moving deeper into the forests and living closer to livestock, making it easier for viruses to jump between species and infect people through proximity, insect bites, and food.
Source: http://washingtontimes.com/world/20040208−105648−7670r.htm

19. *February 09, Associated Press* — **Thailand warns of second bird flu onslaught. A Thai health official said Monday authorities should prepare for the possibility of a second outbreak of bird flu.** Vietnam reported the region's nineteenth fatality from the virus that has ravaged poultry farms across Asia. **The World Health Organization (WHO), meanwhile, said China may already have human cases of bird flu, although the country hasn't reported any.** It said while the government has been sharing information about known

outbreaks, it might not be aware of everything happening in the country. Health authorities in Cambodia are unlikely to know if a woman suspected of having bird flu died from the disease because there were apparently no blood samples taken from her while she was hospitalized. The woman died at a hospital in Vietnam on Friday after falling ill in Cambodia. Charan Trinwuthipong, director general of Thailand's Department of Communicable Disease Control, said the "first wave of bird flu outbreak has passed," in an apparent reference to the country's almost complete cull of poultry in bird flu−affected areas. He said the Agriculture Ministry is trying to eliminate the sources spreading the disease, "but we don't know when the second wave will come, and we don't trust the situation."
Source: http://www.mlive.com/newsflash/lateststories/index.ssf?/base/international−1/1076329441284242.xml

[Return to top]

Government Sector

20. *February 09, Government Computer News* — **DHS launches trio of IT security groups.** The Department of Homeland Security (DHS) has formed three new organizations to strengthen federal IT defenses and coordinate responses to systems threats. **In an exclusive interview, DHS National Cyber Security Division director Amit Yoran said the groups give cybersecurity officials a method for meeting in person as well as in online collaboration environments. Yoran outlined the roles of the three new units:** The Government Forum of Incident Response Teams, or G−FIRST, is made up of frontline systems chiefs. It includes officials from the 24−hour watch center within Yoran's division, the U.S. Computer Emergency Response Team, the Pentagon and civilian agencies. The Chief Information Security Officers Forum was created "to share information about programs that are successful and ones that are challenged and need assistance." Its members are senior officials designated to oversee each agency's cybersecurity and make sure agencies meet the mandates of the Federal Information Security Management. The third unit, the Cyber Interagency Incident Management Group, includes officials from agencies "that have significant capabilities in cybersecurity," Yoran said.
Source: http://www.gcn.com/vol1_no1/daily−updates/24896−1.html

[Return to top]

Emergency Services Sector

21. *February 09, The New York Post* — **New York City firehouses in disrepair. New York's firefighters are living and working in crumbling, rat−infested stations with standing sewage and even fire−code violations, according to an enormous list of problems compiled by the firefighters union.** The Uniformed Firefighters Association submitted a list of problems at the city's 223 houses to the FDNY last April, but Phil McArdle, the union's safety and health officer, says few repairs were made. Almost 50 houses on the list are infested with rats. Exposed electrical wires, a fire hazard, are also common. At Engine 37 in Manhattan, there is exposed wiring throughout the building, including the second floor, which is also missing smoke detectors, according to the UFA list. At Engine 284 in Brooklyn, rust flows from every

faucet in the house. The FDNY says it is spending millions of dollars on repairs. Gribbon said that in the 2005 budget, which starts July 1, there is almost $1 million for a survey of all the city's firehouses, something that hasn't been done in almost 10 years.
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=46&id=25827

22. *February 09, Newswise* — **Advanced strain gauge developed to warn of structural damage.** Following an earthquake, it's often difficult to determine which buildings, roads or bridges have sustained enough structural damage to make them dangerous. Identifying potentially damaged natural gas pipes and pipelines may be even more important. **An advanced optical strain gauge just developed by two University of Rhode Island researchers may be the key to ensuring public safety under these and other circumstances.** Strain is a basic physical measurement, according to the researchers, which is derived by determining thermal displacement −− expansion or contraction due to temperature changes −− or mechanically by determining the displacement when a load is applied. The gauges have been designed to be compatible with fiber optic technology. **The researchers anticipate the gauges will be used primarily in civil structures like buildings, roads and bridges. In earthquake−prone areas, especially, they believe that use of such a device should become required in building codes. A typical home application would cost approximately $100, similar to installation of a common carbon monoxide detector.** In addition, there are a number of specialty uses for the gauges. Aerospace applications include use on airplane wings, landing gear, and other equipment prone to flexing and fatigue.
Source: http://www.newswise.com/articles/view/503149/

[Return to top]

Information and Telecommunications Sector

23. *February 10, Security Wire* — **IPv6 vulnerable to remote denial−of−service attacks. The OpenBSD implementation of IPv6 has a security vulnerability that requires an upgrade to prevent a remote attacker from causing a denial of service**. IPv6 is the successor to IPv4 and is already being implemented by some enterprises, either alone or in parallel with IPv4. While one of the main attractions of IPv6 is its vastly larger address space, administrators are also anticipating security improvements, especially with authentication. However, independent security researcher Georgi Guninski has identified an error in the handling of IPv6 traffic when the host is configured to receive ICMPv6 (Internet Control Message Protocol) and is listening on a TCP port. A remote attacker can take advantage of this by setting a small IPv6 MTU (Maximum Transmission Unit) and then connecting to an open TCP port. This will crash the target system, causing a denial of service **The problem occurs on OpenBSD 3.4. PivX Solutions recommends OpenBSD administrators acquire the revised code from CVS and recompile their kernels**.
Source: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci949128,00.html

24. *February 09, Computerworld* — **Third Mydoom variant discovered in the wild.** Yet another Mydoom variant has been found in the wild. Known as Mydoom.C or SyncZ, the malicious code appears to be scanning the Internet for systems already infected by the original Mydoom. When finding a vulnerable machine, it uploads itself via TCP Port 3127, and creates a copy of

itself in the Windows System directory as "intrenat.exe" as well as several other files in various Windows directories. **This virus, like the Mydoom.B version before it, attempts to find so−called zombie computers to launch a denial−of−service (DoS) attack on Microsoft's Website. However, it does not appear to seek to e−mail itself to other systems**. This latest version is unlikely to affect U.S. corporate networks that successfully defended against the initial MyDoom virus, said Ken Dunham of security consulting company iDefense Inc. However, **with many home, small−business and overseas systems potentially still infected, the worm has the potential of launching a successful DoS attack against the Microsoft.com Website**−−which would affect businesses that need to access that site for patches, updates and other information.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,90005,00.html

25. *February 06, The Register* — **Clueless office workers help spread computer viruses.** Busy or apathetic employees are accelerating the spread of viruses and potentially costing UK businesses millions in clean−up charges, according to a survey released in the Friday. Two−thirds of the 1,000 people quizzed by market researchers TNS in January admit they are not aware of even the most basic virus prevention measures. Meanwhile a third of those polled in the study said they are too busy to check their emails before opening them. **Nine in ten of the workers quizzed believe that have no part to play in preventing the spread of viruses, preferring to leave responsibility to "their IT department, Microsoft or the government."** Over one third of UK workers quizzed feel overwhelmed by the number of emails they get and a third claim to be too busy to check emails before opening them. One in five people surveyed said they are "too busy to download anti−virus updates".
Source: http://www.theregister.co.uk/content/55/35393.html

26. *February 04, CommsDesign.com* — **Security firm warns of holes in Bluetooth mobiles. There are serious flaws in the authentication and data−transfer mechanisms on some top selling Bluetooth−enabled mobile phones, leaving them wide open to hackers**. Security and encryption specialist AL Digital uncovered two specific security breaches. One is the "SNARF attack," where data including phonebook, calendar, associated attachments and business cards can be obtained without the owner's knowledge or consent. The security breach exists on several models from both Nokia and Sony−Ericsson. Another even more invasive problem is "back−door attack." A phone's complete memory contents can be accessed by a previously trusted ("paired") device that has since been removed from the trusted list. This means that not only can data be retrieved from the phone, but other services can be accessed without permission, including modems, Internet, WAP and GPRS gateways.
Source: http://www.techweb.com/wire/story/TWB20040204S0011

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_MYDOOM.A** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	3127 (mydoom), 135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 445 (microsoft−ds), 1433 (ms−sql−s), 27374 (SubSeven), 80 (www), 1080 (socks), 3128 (squid−http) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *February 09, Associated Press* — **Treasury blocks assets of foreigners suspected of obstructing peace accords. The U.S. Department of Treasury on Monday moved to block the financial assets of 13 foreigners suspected of obstructing the Dayton Peace Accords in Bosnia−Herzegovina.** The action by the department's Office of Foreign Assets Control covers Dragan Basevic, Beljko Borovcanin, Samojko Djorda, Ljuban Ecim, Avdyl Jakupi, Radomir Kojic, Tomislav Kovac, Predrag Kujundzic, Milovan Marijanovic, Ivan Sarac, Mirko Saravic, Xhezair Shaqiri and Menduh Thaci. The Dayton Peace Accords that ended the war in 1995 carved the country into a Bosnian Serb republic and a Muslim−Croat federation.
Source: http://biz.yahoo.com/ap/040209/na_fin_us_bosnia_assets_2.htm l

28. *February 09, CNN* — **Police have description of Ohio highway shooter.** Investigators trying to solve a string of highway shootings near Columbus, OH, now have a description of the shooter who fired on two vehicles a day earlier. **The shootings are the latest incidents authorities believed are linked to a string of 21 others southwest of the city since May, including one that was fatal. A passenger in one of the cars attacked Sunday described the shooter as a white male, between 30 and 40 years old, in a small dark car, Franklin County Sheriff Chief Deputy Steve Martin said Sunday. The witness also said the man held a handgun as he stood on the overpass bridge and fired down at the vehicle.** All 21 shootings have been linked, most through ballistics tests. Martin said investigators with the Columbus police crime lab are examining Sunday's evidence. The shootings took place on two different bridges over Interstate 71 in Fayette County, about 35 miles from the intersection of Interstate 71 and Interstate 270, the Columbus beltway. The locations are farther south than any previous shootings. Since May, there have been 21 shootings on or near the southwest corridor of Interstate 270, which circles Columbus. There is a $60,000 reward for information leading to the arrest and indictment of whoever is responsible.
Source: http://www.cnn.com/2004/US/Midwest/02/08/ohio.shootings/inde x.html

29. *February 09, Washington Post* — **Al Qaeda trying to spark a civil war in Iraq, U.S. says.** The al Qaeda terrorist network has been trying to spark a "civil war" in Iraq among religious and ethnic groups in an effort to tear the country apart and prevent a transfer of sovereignty from U.S. occupation authorities to Iraqis, U.S. officials in Baghdad said Monday. **The officials said the plan was outlined in a 17−page letter that appealed to al Qaeda leaders outside Iraq for help in meeting the goals of the network's operatives inside the country.** The letter was found in the possession of a "courier" who was trying to leave the country, officials said. **The document outlines what is "clearly a plan on the part of outsiders to come in this country and spark civil war, create sectarian violence, and try to expose fissures in this society," said Brig. Gen. Mark Kimmitt, a spokesman for the U.S. military in Iraq.** He told a news conference in Baghdad that U.S. authorities believe the document is "credible." Kimmitt said the apparent author of the letter was Abu Musab Zarqawi, a Jordanian who escaped from Afghanistan in 2001 after the fall of the radical Islamic Taliban government.
Source: http://www.washingtonpost.com/wp−dyn/articles/A25736−2004Feb 9.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−3644 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323−3204.

DHS/IAIP Disclaimer